PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-330871

(43)Date of publication of application : 30.11.2000

(51)Int.Cl. G06F 12/14
G11B 20/10
// G09C 1/00

(21)Application number : 11-141269

(22)Date of filing : 21.05.1999

(71)Applicant : VICTOR CO OF JAPAN LTD

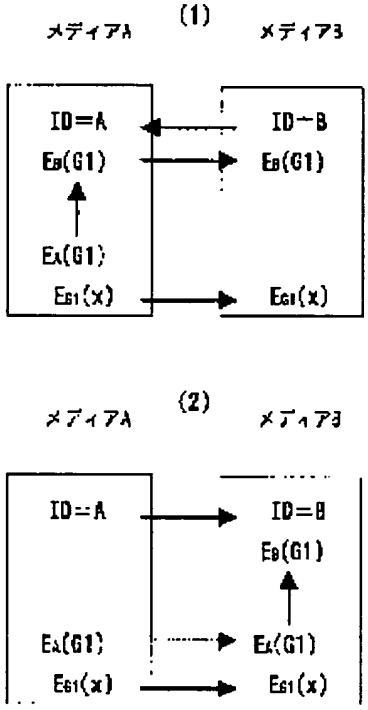
(72)Inventor : SUGAWARA TAKAYUKI

(54) METHOD AND DEVICE FOR RECORDING CONTENTS INFORMATION

(57)Abstract:

PROBLEM TO BE SOLVED: To record contents data by plural users while preventing the unauthorized copy of the contents data.

SOLUTION: In the case of recording ciphered contents information EG1 (x) from a medium A to a medium B, the medium A side reads out the ID=B of the medium B for receiving a copy, deciphers 1st ciphered key information EA (G1) previously ciphered by the ID=A of the medium A, ciphers the deciphered information again by the ID=B of the medium B, and transfers 2nd ciphered key information EB (G1) to the medium B.



LEGAL STATUS

[Date of request for examination] 28.09.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]	
[Patent number]	3682840
[Date of registration]	03.06.2005
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19) 日本国特許庁 (JP)

(12) 公開特許公報（A）

(11) 特許出願公開番号

特開２０００－３３０８７１

（Ｐ２０００－３３０８７１Ａ）

(43) 公開日 平成12年11月30日(2000.11.30)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｂ	5B017
Ｇ１１Ｂ	20/10		Ｇ１１Ｂ	20/10	Ｈ	5D044
// Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｆ	5J104
						9A001

審査請求 未請求 請求項の数 １６ ＯＬ （全 １５ 頁）

(21) 出願番号 特願平11-141269

(22) 出願日 平成11年5月21日(1999.5.21)

(71) 出願人 000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町3丁目12番地

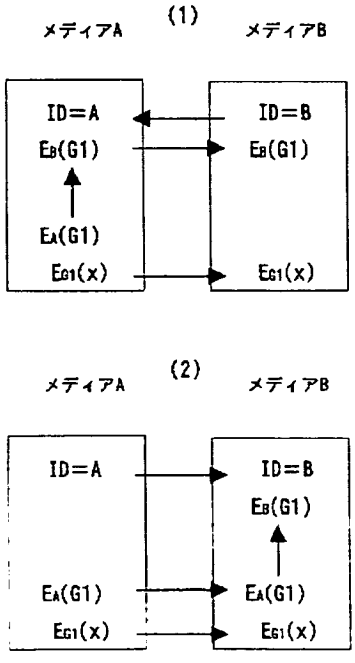
(72) 発明者 菅原 隆幸
神奈川県横浜市神奈川区守屋町3丁目12番地 日本ビクター株式会社内

Ｆターム(参考) 5B017 AA06 BA05 BA07 BB03 BB10 CA16
5D044 AB05 AB07 DE48 GK17 HL06 HL11
5J104 AA16 EA26 JA03 NA02 NA05 NA36 PA10 PA14
9A001 EE03 JZ71 LL03

(54)【発明の名称】コンテンツ情報記録方法及びコンテンツ情報記録装置

(57)【要約】
【課題】 不正なコピーを防止しつつ、コンテンツデータのユーザー間での記録を可能とする。
【解決手段】 暗号化コンテンツ情報ＥG1(X)をメディアＡからメディアＢに記録したときに、メディアＡ側でコピー先メディアのＩＤ＝Ｂを読み取り、先にメディアＡ側でＩＤ＝Ａで暗号化された第１の暗号化鍵情報ＥA(G1)を復号し、コピー先のＩＤ＝Ｂで再暗号化して第２の暗号化鍵情報ＥB(G1)にしてメディアＢに転送する。

図４



1

【特許請求の範囲】

【請求項１】第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録する際に、

前記第１のメディア側から前記第１の暗号化コンテンツ情報を前記第２のメディア側に出力し、

前記第２のメディア側で、前記第１のメディア側から得た前記第１のメディアのＩＤに関する情報により一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化した第２の暗号化コンテンツ情報を前記第２のメディアに記録することを特徴とするコンテンツ情報記録方法。

【請求項２】第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録する際に、

前記第１のメディア側で、一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディア側から得た前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化して第２の暗号化コンテンツ情報を得、その第２の暗号化コンテンツ情報を前記第２のメディア側に出力し、

前記第２のメディア側で、前記第２の暗号化コンテンツ情報を前記第２のメディアに記録することを特徴とするコンテンツ情報記録方法。

【請求項３】第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録する際に、下記方法［ａ］と方法［ｂ］とを選択することを特徴とするコンテンツ情報記録方法。

方法［ａ］

前記第１のメディア側から前記第１の暗号化コンテンツ情報を前記第２のメディア側に出力し、

前記第２のメディア側で、前記第１のメディア側から得た前記第１のメディアのＩＤに関する情報により一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化した第２の暗号化コンテンツ情報を前記第２のメディアに記録する。

方法［ｂ］

前記第１のメディア側で、一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディア側から得た前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化して第２の暗号化コンテンツ情報を得、その第２の暗号化コンテンツ情報を前記第２のメディア側に出力し、

前記第２のメディア側で、前記第２の暗号化コンテンツ

2

情報を前記第２のメディアに記録する。

【請求項４】請求項１～３のいずれか一つに記載のコンテンツ情報記録方法において、

前記第１の暗号化コンテンツ情報のＩＤ鍵は、前記第１のメディアのＩＤをそのまま用いた共通鍵または前記第１のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であり、

前記第２の暗号化コンテンツ情報のＩＤ鍵は、前記第２のメディアのＩＤをそのまま用いた共通鍵または前記第２のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であることを特徴とするコンテンツ情報記録方法。

【請求項５】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録する際に、

前記第１のメディア側から前記暗号化コンテンツ情報と前記第１の暗号化鍵情報とを前記第２のメディア側に出力し、

前記第２のメディア側で、前記暗号化コンテンツ情報を前記第２のメディアに記録すると共に、前記第１のメディア側から得た前記第１のメディアのＩＤに関する情報により一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化した第２の暗号化鍵情報を前記第２のメディアに記録することを特徴とするコンテンツ情報記録方法。

【請求項６】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録する際に、

前記第１のメディア側で、一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディア側から得た前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化して第２の暗号化鍵情報を得、その第２の暗号化鍵情報を前記第２のメディア側に出力し、

前記第２のメディア側で、前記第１のメディア側から出力された前記暗号化コンテンツ情報と前記第２の暗号化鍵情報とを前記第２のメディアに記録することを特徴とするコンテンツ情報記録方法。

【請求項７】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録する際に、下記方法［ａ］と方法［ｂ］とを選択することを特

徴とするコンテンツ情報記録方法。
方法［ａ］
前記第１のメディア側から前記暗号化コンテンツ情報と前記第１の暗号化鍵情報とを前記第２のメディア側に出力し、
前記第２のメディア側で、前記暗号化コンテンツ情報を前記第２のメディアに記録すると共に、前記第１のメディア側から得た前記第１のメディアのＩＤに関する情報により一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化した第２の暗号化鍵情報を前記第２のメディアに記録する。
方法［ｂ］
前記第１のメディア側で、一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディア側から得た前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化して第２の暗号化鍵情報を得、その第２の暗号化鍵情報を前記第２のメディア側に出力し、前記第２のメディア側で、前記第１のメディア側から出力された前記暗号化コンテンツ情報と前記第２の暗号化鍵情報とを前記第２のメディアに記録する。
【請求項８】請求項５～７のいずれか一つに記載のコンテンツ情報記録方法において、
前記所定のコンテンツ鍵は共通鍵もしくは公開鍵であり、
前記第１の暗号化鍵情報のＩＤ鍵は、前記第１のメディアのＩＤをそのまま用いた共通鍵または前記第１のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であり、
前記第２の暗号化鍵情報のＩＤ鍵は、前記第２のメディアのＩＤをそのまま用いた共通鍵または前記第２のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であることを特徴とするコンテンツ情報記録方法。
【請求項９】第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録するコンテンツ情報記録装置であって、
前記第２のメディア側において、前記第１のメディア側から出力された前記第１のメディアのＩＤに関する情報により、前記第１のメディア側から出力された前記第１の暗号化コンテンツ情報の暗号を一旦解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化した第２の暗号化コンテンツ情報を前記第２のメディアに記録させる記録手段を設けたこと特徴とするコンテンツ情報記録装置。
【請求項１０】第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録するコンテンツ情報記録装置であって、
前記第１のメディア側において、一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディア側から出力された前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化して第２の暗号化コンテンツ情報を得、その第２の暗号化コンテンツ情報を前記第２のメディア側に出力させ、前記第２の暗号化コンテンツ情報を前記第２のメディアに記録させる記録手段を設けたことを特徴とするコンテンツ情報記録装置。
【請求項１１】第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録する際に、下記記録動作［ａ］と記録動作［ｂ］とを選択する選択手段を設けたこと特徴とするコンテンツ情報記録装置。
記録動作［ａ］
前記第２のメディア側において、前記第１のメディア側から出力された前記第１のメディアのＩＤに関する情報により、前記第１のメディア側から出力された前記第１の暗号化コンテンツ情報の暗号を一旦解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化した第２の暗号化コンテンツ情報を前記第２のメディアに記録させる。
記録動作［ｂ］
前記第１のメディア側において、一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディア側から出力された前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化して第２の暗号化コンテンツ情報を得、その第２の暗号化コンテンツ情報を前記第２のメディア側に出力させ、前記第２の暗号化コンテンツ情報を前記第２のメディアに記録させる。
【請求項１２】請求項９～１１のいずれか一つに記載のコンテンツ情報記録装置において、
前記第１の暗号化コンテンツ情報のＩＤ鍵は、前記第１のメディアのＩＤをそのまま用いた共通鍵または前記第１のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であり、
前記第２の暗号化コンテンツ情報のＩＤ鍵は、前記第２のメディアのＩＤをそのまま用いた共通鍵または前記第２のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であることを特徴とするコンテンツ情報記録装置。
【請求項１３】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録するコンテンツ情報記録装置であって、

前記第２のメディア側で、前記第１のメディア側から出力された前記第１のメディアのＩＤに関する情報により、前記第１の暗号化鍵情報の暗号を一旦解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化した第２の暗号化鍵情報を前記第２のメディアに記録させる暗号化鍵情報記録手段を設けたことを特徴とするコンテンツ情報記録装置。

【請求項１４】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録するコンテンツ情報記録装置であって、

前記第１のメディア側で、一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディア側から出力された前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化して第２の暗号化鍵情報を得、その第２の暗号化鍵情報を前記第２のメディア側に出力させ、前記第２の暗号化鍵情報を前記第２のメディアに記録させる暗号化鍵情報記録手段を設けたことを特徴とするコンテンツ情報記録装置。

【請求項１５】所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録する際に、下記記録動作［ａ］と記録動作［ｂ］とを選択する選択手段を設けたこと特徴とするコンテンツ情報記録装置。

記録動作［ａ］

前記第２のメディア側で、前記第１のメディア側から出力された前記第１のメディアのＩＤに関する情報により、前記第１の暗号化鍵情報の暗号を一旦解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化した第２の暗号化鍵情報を前記第２のメディアに記録させる。

記録動作［ｂ］

前記第１のメディア側で、一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディア側から出力された前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化して第２の暗号化鍵情報を得、その第２の暗号化鍵情報を前記第２のメディア側に出力させ、前記第２の暗号化鍵情報を前記第２のメディアに記録させる。

【請求項１６】請求項１３～１５のいずれか一つに記載のコンテンツ情報記録装置において、

前記所定のコンテンツ鍵は共通鍵もしくは公開鍵であり、

前記第１の暗号化鍵情報のＩＤ鍵は、前記第１のメディアのＩＤをそのまま用いた共通鍵または前記第１のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であり、

前記第２の暗号化鍵情報のＩＤ鍵は、前記第２のメディアのＩＤをそのまま用いた共通鍵または前記第２のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であることを特徴とするコンテンツ情報記録装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンテンツ情報を記録再生するコンテンツ情報配信システムに関するものである。そして、この発明はコンテンツ情報（特にオーディオやビデオのデータ）を配信し、配信されたデータの不正な譲渡、複製を阻止しながら、ユーザーのメディア間でのデータの譲渡、複製を安全に行うことのできるコンテンツ情報配信システムにおけるコンテンツ情報記録方法及びコンテンツ情報記録装置を提供することを目的としている。

【０００２】

【従来の技術】暗号化技術の発展に伴い、ネットワークを利用してオーディオやビデオのディジタルデータを配信する有用な方法として、特開平１０－２６９２８９号公報に記載のディジタルコンテンツ配布管理方法、ディジタルコンテンツ再生方法及び装置がある。この発明においては、ディジタルコンテンツの配布側では、ディジタルコンテンツを暗号化及び圧縮して加工し、この加工したディジタルコンテンツと暗号化したコンテンツ鍵、さらに暗号化した課金情報を通信相手側に送信し、通信相手から送信されてきたコンテンツ使用情報に基づいて徴収した利用金を権利者に対して分配するようにしている。一方、ディジタルコンテンツの再生側では、その加工されたディジタルコンテンツをコンテンツ鍵にて復号すると共に伸長して再生し、同時にコンテンツの使用に応じて課金情報の減額とコンテンツに使用情報を配布側に送信するようにし、記録されたコンテンツを持ち運びできるようにした。また、特開平９－２５３０３号公報に記載の情報記記録媒体、記録装置、情報伝送システム、暗号解読装置がある。この発明の情報記録媒体は、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録されるにものおいて、上記暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する際の条件情報が記録される。即ち、暗号化鍵情報の制御情報内に、機器情報や領域情報が含まれているため、ユーザ側で暗号化された情報をそのままＨＤＤや光ディスクにコピーし、不正使用をすることを防止した。

【０００３】

【発明が解決しようとする課題】しかしながら上記の従来の方式では、一度メディアに記録されたコンテンツデータを、ユーザー間で譲渡、複製することができない（メディア自体の譲渡はできてもそのメディアに記録さ

れたコンテンツデータの正規の再生ができない。）ので、ユーザーがコンテンツデータを手に入れるためには、一度は必ず課金管理機関、データ管理センター等に接続しなければならない。また、1人のユーザーが複数のメディアを持っていた場合、そのメディア間でデータを移動させることができない。暗号化を解いてコンテンツデータを伝送した場合にはコンテンツデータの譲渡、複製は可能となるが、当然不正な譲渡、複製を許すこととなりデータ伝送のセキュリティを確保できない。本発明は、コンテンツ情報を配信し、配信されたデータの不正な譲渡、複製を阻止しながら、ユーザーのメディア間でのデータの譲渡、複製を安全に行うことのできるコンテンツ情報配信システムにおけるコンテンツ情報記録方法及びコンテンツ情報記録装置を提供することを目的としている。

【０００４】

【課題を解決するための手段】そこで、上記課題を解決するために本発明は、下記の方法、装置を提供するものである。

（１）第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録する際に、前記第１のメディア側から前記第１の暗号化コンテンツ情報を前記第２のメディア側に出力し、前記第２のメディア側で、前記第１のメディア側から得た前記第１のメディアのＩＤに関する情報により一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化した第２の暗号化コンテンツ情報を前記第２のメディアに記録することを特徴とするコンテンツ情報記録方法。

（２）第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録する際に、前記第１のメディア側で、一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディア側から得た前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化して第２の暗号化コンテンツ情報を得、その第２の暗号化コンテンツ情報を前記第２のメディア側に出力し、前記第２のメディア側で、前記第２の暗号化コンテンツ情報を前記第２のメディアに記録することを特徴とするコンテンツ情報記録方法。

（３）第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録する際に、下記方法［ａ］と方法［ｂ］とを選択することを特徴とするコンテンツ情報記録方法。

方法［ａ］

前記第１のメディア側から前記第１の暗号化コンテンツ情報を前記第２のメディア側に出力し、前記第２のメディア側で、前記第１のメディア側から得た前記第１のメディアのＩＤに関する情報により一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化した第２の暗号化コンテンツ情報を前記第２のメディアに記録する。

方法［ｂ］

前記第１のメディア側で、一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディア側から得た前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化して第２の暗号化コンテンツ情報を得、その第２の暗号化コンテンツ情報を前記第２のメディア側に出力し、前記第２のメディア側で、前記第２の暗号化コンテンツ情報を前記第２のメディアに記録する。

（４）上記（１）～（３）のいずれか一つに記載のコンテンツ情報記録方法において、前記第１の暗号化コンテンツ情報のＩＤ鍵は、前記第１のメディアのＩＤをそのまま用いた共通鍵または前記第１のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であり、前記第２の暗号化コンテンツ情報のＩＤ鍵は、前記第２のメディアのＩＤをそのまま用いた共通鍵または前記第２のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であることを特徴とするコンテンツ情報記録方法。

（５）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録する際に、前記第１のメディア側から前記暗号化コンテンツ情報と前記第１の暗号化鍵情報とを前記第２のメディア側に出力し、前記第２のメディア側で、前記暗号化コンテンツ情報を前記第２のメディアに記録すると共に、前記第１のメディア側から得た前記第１のメディアのＩＤに関する情報により一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化した第２の暗号化鍵情報を前記第２のメディアに記録することを特徴とするコンテンツ情報記録方法。

（６）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録する際に、前記第１のメディア側で、一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディア側から得た前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテ

ンツ鍵を再暗号化して第２の暗号化鍵情報を得、その第２の暗号化鍵情報を前記第２のメディア側に出力し、前記第２のメディア側で、前記第１のメディア側から出力された前記暗号化コンテンツ情報と前記第２の暗号化鍵情報とを前記第２のメディアに記録することを特徴とするコンテンツ情報記録方法。

（７）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録する際に、下記方法［ａ］と方法［ｂ］とを選択することを特徴とするコンテンツ情報記録方法。

方法［ａ］

前記第１のメディア側から前記暗号化コンテンツ情報と前記第１の暗号化鍵情報とを前記第２のメディア側に出力し、前記第２のメディア側で、前記暗号化コンテンツ情報を前記第２のメディアに記録すると共に、前記第１のメディア側から得た前記第１のメディアのＩＤに関する情報により一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化した第２の暗号化鍵情報を前記第２のメディアに記録する。

方法［ｂ］

前記第１のメディア側で、一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディア側から得た前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化して第２の暗号化鍵情報を得、その第２の暗号化鍵情報を前記第２のメディア側に出力し、前記第２のメディア側で、前記第１のメディア側から出力された前記暗号化コンテンツ情報と前記第２の暗号化鍵情報とを前記第２のメディアに記録する。

（８）上記（５）～（７）のいずれか一つに記載のコンテンツ情報記録方法において、前記所定のコンテンツ鍵は共通鍵もしくは公開鍵であり、前記第１の暗号化鍵情報のＩＤ鍵は、前記第１のメディアのＩＤをそのまま用いた共通鍵または前記第１のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であり、前記第２の暗号化鍵情報のＩＤ鍵は、前記第２のメディアのＩＤをそのまま用いた共通鍵または前記第２のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であることを特徴とするコンテンツ情報記録方法。

（９）第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録するコンテンツ情報記録装置であって、前記第２のメディア側において、前記第１のメディア側から出力された前記第１のメディアのＩＤに関する情報により、前記第１のメディア側から出力された前記第１の暗号化コンテンツ情報の暗号を一旦解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化した第２の暗号化コンテンツ情報を前記第２のメディアに記録させる記録手段を設けたこと特徴とするコンテンツ情報記録装置。

（１０）第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録するコンテンツ情報記録装置であって、前記第１のメディア側において、一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディア側から出力された前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化して第２の暗号化コンテンツ情報を得、その第２の暗号化コンテンツ情報を前記第２のメディア側に出力させ、前記第２の暗号化コンテンツ情報を前記第２のメディアに記録させる記録手段を設けたことを特徴とするコンテンツ情報記録装置。

（１１）第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録する際に、下記記録動作［ａ］と記録動作［ｂ］とを選択する選択手段を設けたこと特徴とするコンテンツ情報記録装置。

記録動作［ａ］

前記第２のメディア側において、前記第１のメディア側から出力された前記第１のメディアのＩＤに関する情報により、前記第１のメディア側から出力された前記第１の暗号化コンテンツ情報の暗号を一旦解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化した第２の暗号化コンテンツ情報を前記第２のメディアに記録させる。

記録動作［ｂ］

前記第１のメディア側において、一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディア側から出力された前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化して第２の暗号化コンテンツ情報を得、その第２の暗号化コンテンツ情報を前記第２のメディア側に出力させ、前記第２の暗号化コンテンツ情報を前記第２のメディアに記録させる。

（１２）上記（９）～（１１）のいずれか一つに記載のコンテンツ情報記録装置において、前記第１の暗号化コンテンツ情報のＩＤ鍵は、前記第１のメディアのＩＤをそのまま用いた共通鍵または前記第１のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であり、前記第２の暗号化コンテンツ情報のＩＤ鍵は、前記第２のメディアのＩＤをそのまま用いた共通鍵または前記第２のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であることを特徴とするコンテンツ情報記録装置。

（１３）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録するコンテンツ情報記録装置であって、前記第２のメディア側で、前記第１のメディア側から出力された前記第１のメディアのＩＤに関する情報により、前記第１の暗号化鍵情報の暗号を一旦解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化した第２の暗号化鍵情報を前記第２のメディアに記録させる暗号化鍵情報記録手段を設けたことを特徴とするコンテンツ情報記録装置。

（１４）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録するコンテンツ情報記録装置であって、前記第１のメディア側で、一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディア側から出力された前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化して第２の暗号化鍵情報を得、その第２の暗号化鍵情報を前記第２のメディア側に出力させ、前記第２の暗号化鍵情報を前記第２のメディアに記録させる暗号化鍵情報記録手段を設けたことを特徴とするコンテンツ情報記録装置。

（１５）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録する際に、下記記録動作［ａ］と記録動作［ｂ］とを選択する選択手段を設けたこと特徴とするコンテンツ情報記録装置。

記録動作［ａ］前記第２のメディア側で、前記第１のメディア側から出力された前記第１のメディアのＩＤに関する情報により、前記第１の暗号化鍵情報の暗号を一旦解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化した第２の暗号化鍵情報を前記第２のメディアに記録させる。

記録動作［ｂ］

前記第１のメディア側で、一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディア側から出力された前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化して第２の暗号化鍵情報を得、その第２の暗号化鍵情報を前記第２のメディア側に出力させ、前記第２の暗号化鍵情報を前記第２のメディアに記録させる。

（１６）上記（１３）～（１５）のいずれか一つに記載のコンテンツ情報記録装置において、前記所定のコンテンツ鍵は共通鍵もしくは公開鍵であり、前記第１の暗号化鍵情報のＩＤ鍵は、前記第１のメディアのＩＤをそのまま用いた共通鍵または前記第１のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であり、前記第２の暗号化鍵情報のＩＤ鍵は、前記第２のメディアのＩＤをそのまま用いた共通鍵または前記第２のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であることを特徴とするコンテンツ情報記録装置。

【０００５】

【発明の実施の形態】本発明によれば、不正な譲渡、複製を防止しつつ、メディアに記録されたコンテンツデータをユーザー間で譲渡、複製することを可能とし、必ずしも課金管理機関、データ管理センター等に接続しなくともユーザーがコンテンツデータを手に入れることを可能とする。また、本発明によれば、1人のユーザーが複数のメディアを持っていた場合、そのメディア間でデータの譲渡、複製を行えるシステムを提供できる。さらには、常に暗号化されたセキュリティの高い状態でコンテンツデータを譲渡、複製することができる。

【０００６】本発明では、

（１）第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録する際に、前記第１のメディア側から前記第１の暗号化コンテンツ情報を前記第２のメディア側に出力し、前記第２のメディア側で、前記第１のメディア側から得た前記第１のメディアのＩＤに関する情報により一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化した第２の暗号化コンテンツ情報を前記第２のメディアに記録するようにした。

（２）第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録する際に、前記第１のメディア側で、一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディア側から得た前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化して第２の暗号化コンテンツ情報を得、その第２の暗号化コンテンツ情報を前記第２のメディア側に出力し、前記第２のメディア側で、前記第２の暗号化コンテンツ情報を前記第２のメディアに記録するようにした。

（３）第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録する際に、下記方法［ａ］と方法［ｂ］とを選択するようにした。

方法［ａ］

前記第１のメディア側から前記第１の暗号化コンテンツ情報を前記第２のメディア側に出力し、前記第２のメディア側で、前記第１のメディア側から得た前記第１のメディアのＩＤに関する情報により一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化した第２の暗号化コンテンツ情報を前記第２のメディアに記録する。

方法［ｂ］

前記第１のメディア側で、一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディア側から得た前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化して第２の暗号化コンテンツ情報を得、その第２の暗号化コンテンツ情報を前記第２のメディア側に出力し、前記第２のメディア側で、前記第２の暗号化コンテンツ情報を前記第２のメディアに記録する。

（４）上記（１）～（３）のいずれか一つに記載のコンテンツ情報記録方法において、前記第１の暗号化コンテンツ情報のＩＤ鍵は、前記第１のメディアのＩＤをそのまま用いた共通鍵または前記第１のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であり、前記第２の暗号化コンテンツ情報のＩＤ鍵は、前記第２のメディアのＩＤをそのまま用いた共通鍵または前記第２のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であるようにした。

（５）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録する際に、前記第１のメディア側から前記暗号化コンテンツ情報と前記第１の暗号化鍵情報とを前記第２のメディア側に出力し、前記第２のメディア側で、前記暗号化コンテンツ情報を前記第２のメディアに記録すると共に、前記第１のメディア側から得た前記第１のメディアのＩＤに関する情報により一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化した第２の暗号化鍵情報を前記第２のメディアに記録するようにした。

（６）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録する際に、前記第１のメディア側で、一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディア側から得た前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化して第２の暗号化鍵情報を得、その第２の暗号化鍵情報を前記第２のメディア側に出力し、前記第２のメディア側で、前記第１のメディア側から出力された前記暗号化コンテンツ情報と前記第２の暗号化鍵情報とを前記第２のメディアに記録するようにした。

（７）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録する際に、下記方法［ａ］と方法［ｂ］とを選択するようにした。

方法［ａ］

前記第１のメディア側から前記暗号化コンテンツ情報と前記第１の暗号化鍵情報とを前記第２のメディア側に出力し、前記第２のメディア側で、前記暗号化コンテンツ情報を前記第２のメディアに記録すると共に、前記第１のメディア側から得た前記第１のメディアのＩＤに関する情報により一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化した第２の暗号化鍵情報を前記第２のメディアに記録する。

方法［ｂ］

前記第１のメディア側で、一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディア側から得た前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化して第２の暗号化鍵情報を得、その第２の暗号化鍵情報を前記第２のメディア側に出力し、前記第２のメディア側で、前記第１のメディア側から出力された前記暗号化コンテンツ情報と前記第２の暗号化鍵情報とを前記第２のメディアに記録する。

（８）上記（５）～（７）のいずれか一つに記載のコンテンツ情報記録方法において、前記所定のコンテンツ鍵は共通鍵もしくは公開鍵であり、前記第１の暗号化鍵情報のＩＤ鍵は、前記第１のメディアのＩＤをそのまま用いた共通鍵または前記第１のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であり、前記第２の暗号化鍵情報のＩＤ鍵は、前記第２のメディアのＩＤをそのまま用いた共通鍵または前記第２のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であるようにした。

（９）第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録するコンテンツ情報記録装置であって、前記第２のメディア側において、前記第１のメディア側から出力された前記第１のメディアのＩＤに関する情報により、前記第１のメディア側から出力された前記第１の暗号化コンテンツ情報の暗号を一旦解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化した第２の暗号化コンテンツ情報を前記第２のメディアに記録させる記録手段を設けるようにした。

（１０）第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録するコンテンツ情報記録装置であって、前記第１のメディア側において、一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディア側から出力された前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化して第２の暗号化コンテンツ情報を得、その第２の暗号化コンテンツ情報を前記第２のメディア側に出力させ、前記第２の暗号化コンテンツ情報を前記第２のメディアに記録させる記録手段を設けるようにした。

（１１）第１のメディアのＩＤに関する情報をＩＤ鍵としてコンテンツ情報を暗号化した第１の暗号化コンテンツ情報が記録された前記第１のメディアから、前記コンテンツ情報を第２のメディアに記録する際に、下記記録動作［ａ］と記録動作［ｂ］とを選択する選択手段を設けるようにしたコンテンツ情報記録装置。

記録動作［ａ］

前記第２のメディア側において、前記第１のメディア側から出力された前記第１のメディアのＩＤに関する情報により、前記第１のメディア側から出力された前記第１の暗号化コンテンツ情報の暗号を一旦解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化した第２の暗号化コンテンツ情報を前記第２のメディアに記録させる。

記録動作［ｂ］

前記第１のメディア側において、一旦前記第１の暗号化コンテンツ情報の暗号を解き、前記第２のメディア側から出力された前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ情報を再暗号化して第２の暗号化コンテンツ情報を得、その第２の暗号化コンテンツ情報を前記第２のメディア側に出力させ、前記第２の暗号化コンテンツ情報を前記第２のメディアに記録させる。

（１２）上記（９）～（１１）のいずれか一つに記載のコンテンツ情報記録装置において、前記第１の暗号化コンテンツ情報のＩＤ鍵は、前記第１のメディアのＩＤをそのまま用いた共通鍵または前記第１のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であり、前記第２の暗号化コンテンツ情報のＩＤ鍵は、前記第２のメディアのＩＤをそのまま用いた共通鍵または前記第２のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であるようにした。

（１３）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録するコンテンツ情報記録装置であって、前記第２のメディア側で、

前記第１のメディア側から出力された前記第１のメディアのＩＤに関する情報により、前記第１の暗号化鍵情報の暗号を一旦解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化した第２の暗号化鍵情報を前記第２のメディアに記録させる暗号化鍵情報記録手段を設けるようにした。

（１４）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録するコンテンツ情報記録装置であって、前記第１のメディア側で、一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディア側から出力された前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化して第２の暗号化鍵情報を得、その第２の暗号化鍵情報を前記第２のメディア側に出力させ、前記第２の暗号化鍵情報を前記第２のメディアに記録させる暗号化鍵情報記録手段を設けるようにした。

（１５）所定のコンテンツ鍵で暗号化された暗号化コンテンツ情報と、前記コンテンツ鍵を第１のメディアのＩＤに関する情報をＩＤ鍵として暗号化した第１の暗号化鍵情報とが記録された前記第１のメディアから、前記暗号化コンテンツ情報を第２のメディアに記録する際に、下記記録動作［ａ］と記録動作［ｂ］とを選択する選択手段を設けるようにしたコンテンツ情報記録装置。

記録動作［ａ］

前記第２のメディア側で、前記第１のメディア側から出力された前記第１のメディアのＩＤに関する情報により、前記第１の暗号化鍵情報の暗号を一旦解き、前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化した第２の暗号化鍵情報を前記第２のメディアに記録させる。

記録動作［ｂ］

前記第１のメディア側で、一旦前記第１の暗号化鍵情報の暗号を解き、前記第２のメディア側から出力された前記第２のメディアのＩＤに関する情報をＩＤ鍵として前記コンテンツ鍵を再暗号化して第２の暗号化鍵情報を得、その第２の暗号化鍵情報を前記第２のメディア側に出力させ、前記第２の暗号化鍵情報を前記第２のメディアに記録させる。

（１６）上記（１３）～（１５）のいずれか一つに記載のコンテンツ情報記録装置において、前記所定のコンテンツ鍵は共通鍵もしくは公開鍵であり、前記第１の暗号化鍵情報のＩＤ鍵は、前記第１のメディアのＩＤをそのまま用いた共通鍵または前記第１のメディアのＩＤを所定の関数により変換した情報を用いた共通鍵であり、前記第２の暗号化鍵情報のＩＤ鍵は、前記第２のメディアのＩＤをそのまま用いた共通鍵または前記第２のメディアのＩＤを所定の関数により変換した情報を用いた共通

鍵であるようにした。

【０００７】まず、図２を用いて本発明の一実施例の構成を説明する。メディアはメディア固有のIDが設定され、メディア制御器にセットすることが出来る。メディアは記録再生可能であり、固有のIDを設定可能なものであれば、固体メモリーやディスク、テープ等でも良い。但し、ID情報が所定の耐タンパー性をもつことが条件である。即ち、IDや暗号化に必要な鍵の保管に対して不正に情報を読み出したり、書き換えたりするのが難しい状態になっていることが望ましい。

【０００８】もっとも簡単なものはメモリータイプでこのメモリーカードは所定のメモリー制御器を介してしか、IDや暗号化鍵情報が引き出せない仕組みになっているものが、安全で簡単に作成できる。メモリーカードは、工場生産時にカード毎に固有なIDが記録されている。もしくは発行装置により発行される際に、そのメモリー固有のIDをＥＥＰＲＯＭなどに記録された後、樹脂封入等で埋めこまれるようになっている。これにより、後からユーザ対応鍵情報が変更できない、つまり不正改ざんできないようにする。メディアには一部のデータのみメディア間のコピーを行うことの出来るメディアパスを有している。

【０００９】メディア制御器はメディアをセットして、PCもしくは専用器などの端末に接続し、メディア内のデータと、端末とのインターフェース機能と、所定のIDでのデータの暗号化、復号化機能を有する。メディア制御器は端末側からメモリーの内部を不正にアクセスできない耐タンパー性をもっている。端末は外部にあるコンテンツ情報を配信をするセンター（配信センター）に接続し、課金、認証など所定の手続きを経て、コンテンツデータを受信する。センターとの接続はインターネットなどのネットワークはもちろん、ISDNや放送、ケーブルTV、PHSなどの無線接続でもかまわない。

【００１０】コンテンツ情報は基本的にコンテンツ毎に違う鍵（コンテンツ鍵）で暗号化される。コンテンツはMPEGなどの所定の圧縮方式によって圧縮された後、DESなどの暗号化がなされている。例えばDESの場合、暗号化鍵は６４ビット程度である。データベースとセンターと端末の関係を図１に示す。センターに設置したデータベースで、コンテンツ情報が、コンテンツX1を暗号化鍵G1で暗号化し、また、違うコンテンツX2を暗号化鍵G2で暗号化するものとして管理されている。

【００１１】このセンターには複数の端末がネットワークで接続されている。端末への送信もセキュリティーを考えて公開鍵方式で暗号化して送信する。ここで端末１（T1）の公開鍵をT1Pとし、復号鍵をT1Dとすると、データベース１に管理されていたコンテンツX1は、暗号化鍵G1で暗号化されＥG1(X1)という暗号化コンテンツ情報とされる。暗号化鍵G1は、端末T1に送信するために端末T1の公開鍵T1Pを使用して暗号化され、暗号化鍵の情報ＥT1P(G1)となる。そして、暗号化コンテンツ情報ＥG1(X1)と暗号化鍵の情報ＥT1P(G1)との２つの情報を端末１(T1)に送信する。

【００１２】端末１でこのコンテンツ情報を再生するためには、端末１の復号鍵T1Dを用いて、暗号化鍵の情報ＥT1P(G1)を復号し、暗号化鍵G1を得て、その暗号化鍵G1で暗号化コンテンツ情報ＥG1(X1)を復号し、コンテンツX1を得て、MPEGなどの復号を行うことで再生することが出来るが、ここでは、送信されたデータを端末で再生することなく、すぐに端末に接続されたメディアに記録することを前提とする。ここでは公開鍵を使って端末までのデータ送信を説明したが、これは、共通鍵方式であっても、また他の方式であっても本発明はサポートすることが出来る。

【００１３】次に図３、４、５を用いて本発明のコンテンツ情報と鍵情報の受け渡し機能について説明する。最初に配信センターから端末T1側のメディアA（第１のメディア）にコンテンツデータを受信する場合を説明する。まず、メディアAをメディア制御器にセットする。メディア制御器を端末Ｔ１にセットして、「データ記録モード」にする。課金、認証など所定の手続きを行う。手続きが終了すると、センターからコンテンツデータが所定の暗号化鍵G1で暗号化されて端末に配信されてくる。

【００１４】即ち、コンテンツXを暗号化鍵G1で暗号化した暗号化コンテンツ情報ＥG1(X)が送信されてくる。また、暗号化鍵G1を端末T1に送信するために、端末T1の公開鍵T1Pを使用して暗号化鍵G1を暗号化した暗号化鍵情報ＥT1P(G1)が端末T1に送信されてくる。端末で復号に使用する鍵はT1Dなので、この暗号化鍵情報ＥT1P(G1)は復号鍵T1Dで復号できる。この状態をＥT1D（G1）と表現する。端末ではこの暗号化鍵情報ＥT1D（G1）を一度復号鍵T1Dで復号して暗号化鍵G1を得る。復号した暗号化鍵G1でコンテンツデータXを復号し、このコンテンツデータXをメディアＡに転送する。

【００１５】メディアにおいてコンテンツをメディアのＩＤによって暗号化し直す方式について図３を用いて説明する。メディア制御器はこのコンテンツデータXを受信したら、メディア制御器内部でメディアＡのＩＤをＩＤ鍵として暗号化し直す。メディアＡには第１の暗号化コンテンツ情報ＥA(X)が記録される。この暗号化コンテンツデータをそのまま、メディアＢにコピーしてもメディアＢではＩＤ＝Ｂであるので、このEA(X)を再生することは出来ない。しかしながら、メディアＡで復号して、再生できる状態の生信号データをメディアＢへ転送するのはセキュリティ上問題がある。

【００１６】そこで、図３（１）のようにメディアＡ側でコピー先メディアのＩＤ＝Ｂを読み取り、先にメディアＡ側でＩＤ＝ＡをＩＤ鍵として暗号化されたコンテンツデータを復号し、コピー先のＩＤ＝ＢをＩＤ鍵として

再暗号化して第２の暗号化コンテンツ情報ＥＢ（Ｘ）としてメディアＢに転送する。

【００１７】もしくは、図３（２）のようにＩＤ＝Ａで暗号化されたコンテンツデータＥＡ（Ｘ）を、そのままメディアＢへ転送し、メディアＢ側で、コピー元のメディアＡのＩＤを読み取り、ＩＤ＝Ａで暗号化されたコンテンツデータを復号し、ＩＤ＝Ｂで再暗号化してＥＢ（Ｘ）として記録する。これにより、コンテンツデータはどちらかのＩＤで暗号化されている状態で転送されるのでセキュリティが確保される。なお、一つの記録装置において、図３（１）に示す方法と図３（２）に示す方法とのどちらか一方を任意に選択できるようにしてもよい。

【００１８】次に、コンテンツ鍵（暗号化鍵）で暗号化された暗号化コンテンツ情報と、これに使用したコンテンツ鍵（暗号化鍵）をさらにそのメディアもしくは端末のIDに関する情報をID鍵として暗号化している場合について図４を用いて説明する。最初に配信センターから端末T1側のメディアA（第１のメディア）にコンテンツデータを受信する場合を説明する。まず、メディアAをメディア制御器にセットする。メディア制御器を端末Ｔ１にセットして、「データ記録モード」にする。課金、認証など所定の手続きを行う。手続きが終了すると、センターからコンテンツデータが所定の暗号化鍵G1で暗号化されて端末に配信されてくる。

【００１９】即ち、コンテンツXを暗号化鍵G1で暗号化した暗号化コンテンツ情報ＥG1(X)が送信されてくる。また、暗号化鍵G1を端末T1に送信するために、端末T1の公開鍵T1Pを使用して暗号化鍵G1を暗号化した暗号化鍵情報ＥT1P(G1)が端末T1に送信されてくる。端末で復号に使用する鍵はT1Dなので、この暗号化鍵情報ＥT1P(G1)は復号鍵T1Dで復号できる。この状態をＥT1D（G1）と表現する。端末ではこの暗号化鍵情報ＥT1D（G1）を一度復号鍵T1Dで復号して暗号化鍵G1を得る。

【００２０】メディア制御器ではこのデータを受信し、メディアAには暗号化コンテンツ情報ＥG1(X)が記録され、同時にメディア制御器はセットされたメディアのIDを認識して、この鍵G1をメディアAの固有のIDであるAという値で再暗号化して第１の暗号化鍵情報ＥA(G1)得、これをメディアAに記録する。このときのデータ構造例を図５に示す。暗号化コンテンツ情報のヘッダーに６４ビットの暗号化鍵情報が記録される。この構造は必ずしも、一体化している必要はなく、対になっていることが管理できれば分離されていてもかまわない。

【００２１】この第１の暗号化鍵情報ＥA(G1)をそのままメディアＢにコピーしても、メディアＢではＩＤ＝Ｂであるので、このＥA(G1)を復号することは出来ない。そこで、図４（１）のようにメディアＡ側でコピー先メディアのＩＤ＝Ｂを読み取り、先にメディアＡ側でＩＤ＝Ａで暗号化された第１の暗号化鍵情報ＥA(G1)を復号し、コピー先のＩＤ＝Ｂで再暗号化して第２の暗号化鍵情報ＥB(G1)にしてメディアＢに転送する。もしくは図４（２）のようにＩＤ＝Ａで暗号化された第１の暗号化鍵情報ＥA(G1)を、そのままメディアＢへ転送し、メディアＢ側で、コピー元のメディアＡのＩＤを読み取り、ＩＤ＝Ａで暗号化された第１の暗号化鍵情報ＥA(G1)を復号し、ＩＤ＝Ｂで再暗号化して第２の暗号化鍵情報ＥB(G1)にして記録する。

【００２２】このように、コンテンツデータが暗号化されている状態ＥG1(X)で転送されるばかりでなく、暗号化鍵Ｇ１もどちらかのメディアのＩＤで暗号化されている状態（ＥA(G1)またはＥB(G1)）で転送されるのでセキュリティが確保される。コンテンツデータＸの容量が大きい場合、図４に示すように、暗号化コンテンツ情報ＥG1(X)の暗号化鍵（コンテンツ鍵）Ｇ１をさらにそのメディアもしくは端末のIDに関する情報をID鍵として暗号化する方式（ＥA(G1)またはＥB(G1)を用いる方式）を用いたほうが、鍵情報だけを復号化、暗号化するだけでコピーできるので、高速にハンドリングが可能である。なお、一つの記録装置において、図４（１）に示す方法と図４（２）に示す方法とのどちらか一方を任意に選択できるようにしてもよい。

【００２３】次に、図６を用いて本発明のコンテンツ情報記録装置の一実施例のブロック図について説明する。このブロック図は暗号化鍵（コンテンツ鍵）Ｇ１をさらにそのメディアもしくは端末のIDに関する情報をID鍵として暗号化する方式（ＥA(G1)またはＥB(G1)を用いる方式）によるものであり、図４（１）のメディアＡからメディアＢへの記録を例に説明する。

【００２４】最初に配信センターからメディアAにコンテンツデータを受信する場合を説明する。まず、メディアAをメディア制御器２１にセットする。メディア制御器２１を端末Ｔ１にセットして、外部インターフェースよりメディア制御器２１のモード設定部５１に「データ記録モード」を設定する。課金、認証など所定の手続きが終了すると、センターからコンテンツデータＸが所定の暗号化鍵Ｇ１で暗号化されて暗号化コンテンツ情報ＥG1（X）として端末Ｔ１に配信されてくる。「データ記録モード」の場合、モード設定部５１はスイッチ１とスイッチ２を鍵暗号化部５２に接続するように切り替える。

【００２５】センターからは、暗号化コンテンツ情報ＥG1（X）と共に、暗号化鍵G1を端末T1に送信するためにT1の公開鍵T1Pを使用して暗号化鍵G1を暗号化したＥT1P(G1)が送信されてくる。端末Ｔ１で復号に使用する鍵はT1Dなのでこの暗号化鍵情報ＥT1P(G1)はT1Dで復号できる。この状態をＥT1D（G1）と表現する。端末Ｔ１ではこの暗号化鍵情報ＥT1D（G1）を一度T1Dで復号する。

【００２６】メディア制御器２１ではこのデータを受信し、メディアAにはこのＥG1(X)が記録され、メディア制

御器２１はセットされたメディアＡのIDをメディアＩＤ読み取り部５３で認識して、鍵暗号化部５２で暗号化鍵Ｇ１をＩＤ＝Ａで暗号化し、暗号化鍵情報ＥＡ(G1)を暗号化鍵情報書き込み部５４に送信する。暗号化鍵情報書き込み部５４では、暗号化鍵情報を、メディアＡに記録されている暗号化コンテンツ情報ＥG1（X）のヘッダー６４ビットに記録する。

【００２７】次に、メディアAに記録されている暗号化コンテンツ情報ＥG1(X)を再生する場合を説明する。メディアAをメディア制御器２１にセットし、外部インターフェースよりメディア制御器２１のモード設定部５１に「データ再生モード」を設定する。メディアＡ側のメディアID発生部３１により発生された信号は、メディア制御器２１のメディアID読み取り部５３によってメディアのID=Aを検出し、暗号化復号部５６に送信する。

【００２８】メディア制御部２１はメディアＡのメモリー部３２から暗号化コンテンツ情報ＥG1(X)を読み出し、暗号化鍵情報読み取り部５５に送信する。暗号化鍵情報読み取り部５５は、先頭にある暗号化鍵情報６４ビットを読み、スイッチ１を介して暗号化鍵情報ＥA(G1)を暗号化鍵復号部５６へ送信する。モード設定部５１によって「データ再生モード」の場合、スイッチ１は暗号化鍵復号部５６側へ切り替えられている。

【００２９】暗号化鍵復号部５６では、入力されたメディアID＝Ａを使用して、暗号化鍵情報ＥA(G1)を復号する。復号した暗号化鍵Ｇ１は暗号化コンテンツデータ復号部５７に送信される。また、暗号化鍵情報読み取り部５５でヘッダーが取り去られた暗号化コンテンツデータは暗号化コンテンツデータ復号部５７に送信される。暗号化コンテンツデータ復号部５７では、入力された暗号化コンテンツデータＥG1(X)と暗号化鍵Ｇ１によって暗号化コンテンツデータを復号化し、再生データとして出力する。

【００３０】次に、メディアAからメディアBへコンテンツデータをコピーする場合を説明する。コンテンツの記録されているコピー元メディアAからコピー先メディアBに暗号化コンテンツ情報ＥG1（X）をコピーする場合、まず、メディア制御器２１にメディアAをセットする。外部インターフェースよりメディア制御器２１のモード設定部５１に「データコピー出力モード」を設定する。

【００３１】メディアＡのメディアID発生部３１により発生された信号は、メディア制御器２１のメディアID読み取り部２３によってメディアのＩＤ＝Ａが検出さし、暗号化鍵復号部５６に送信される。モード設定部５１に「データコピー出力モード」と設定されているとき、スイッチ１、２は、暗号化鍵復号部５６につながるように切り替えられている。

【００３２】メディアＡに記録されていた暗号化コンテンツ情報ＥG1（X）は暗号化鍵情報読み取り部５５に送信され、ここでヘッダー６４ビットの暗号化鍵情報ＥA(G1)が読み取られる。読み取られた暗号化鍵情報ＥA(G1)は暗号化鍵復号部５６に送信される。暗号化鍵復号部５６では、入力されたＩＤ＝Ａと暗号化鍵情報ＥA(G1)から暗号化鍵Ｇ１を復号し、鍵メモリー５８に一時記録する。

【００３３】一方、暗号化コンテンツデータＥG1（X）は、メディアＡ側のメモリー部３２のデータ移動用領域に格納され、メディアバス３３を介して、メディアバス３３に接続されるメディアBに高速に転送される。このメディアバスは、メディアAとメディアBを物理的に連結してデータ転送する。転送するデータ自体は暗号化コンテンツデータのみがこのメディアバスを通過できるようになっているので安全性が高い。

【００３４】次に、メディア制御器２１にメディアBをセットする。メディア制御器２１のメディアID読み取り部５３によってメディアのID＝Ｂを検出する。モード設定部５１に「データコピー入力モード」と設定されているとき、スイッチ１、２は鍵暗号化部５２につながるように切り替えられている。鍵暗号化部５２では、鍵メモリー５８から暗号化鍵Ｇ１を読み出し、メディアＩＤ読み取り部５３から入力されたＩＤ＝Ｂを使用して、暗号化鍵Ｇ１をＩＤ＝Ｂで暗号化しEB(G1)とする。暗号化鍵情報ＥB(G1)は暗号化鍵情報書き込み部５４に送信される。暗号化鍵情報ＥB(G1)はメディアＢのメモリー部３２Ｂに記録される。

【００３５】メディアＢに記録された暗号化コンテンツ情報ＥG1（X）を再生する場合を説明する。これはメディアＡに記録された暗号化コンテンツ情報ＥG1（X）を再生する場合と同じである。即ち、メディアＢをメディア制御器２１にセットし、外部インターフェースよりメディア制御器２１のモード設定部５１に「データ再生モード」を設定する。メディアＢ側のメディアID発生部３１Ｂにより発生された信号は、メディア制御器２１のメディアID読み取り部５３によってメディアのID=Bを検出し、暗号化復号部５６に送信する。

【００３６】メディア制御部２１はメディアＢのメモリー部３２Ｂから暗号化コンテンツ情報ＥG1(X)を読み出し、暗号化鍵情報読み取り部５５に送信する。暗号化鍵情報読み取り部５５は、先頭にある暗号化鍵情報６４ビットを読み、スイッチ１を介して暗号化鍵情報ＥB(G1)を暗号化鍵復号部５６へ送信する。モード設定部５１によって「データ再生モード」の場合、スイッチ１は暗号化鍵復号部５６側へ切り替えられている。

【００３７】暗号化鍵復号部５６では、入力されたメディアID＝Bを使用して、暗号化鍵情報ＥB(G1)を復号する。復号した暗号化鍵Ｇ１は暗号化コンテンツデータ復号部５７に送信される。また、暗号化鍵情報読み取り部５５でヘッダーが取り去られた暗号化コンテンツデータは暗号化コンテンツデータ復号部５７に送信される。暗号化コンテンツデータ復号部５７では、入力された暗号

化コンテンツデータＥG1(X)と暗号化鍵Ｇ１によって暗号化コンテンツデータを復号化し、再生データとしてコンテンツデータＸを出力する。

【００３８】このように、本実施例の記録装置では、コンテンツデータが暗号化されている状態ＥG1(X)で転送されるばかりでなく、暗号化鍵Ｇ１もメディアＢのＩＤで暗号化されている状態（ＥB(G1)）で転送されるのでセキュリティが確保される。上記実施例では、暗号化鍵Ｇ１を復号化しメディアＢのＩＤで再暗号化する処理を送信側（メディアＡ側）で行った。よって、受信専用のメディア制御器にはを鍵暗号化部５２、スイッチ１、２は不要となり、システムとして限定されたユーザーのみ送信できるというシステムを構築することが可能となる。

【００３９】なお、メディアＡからメディアＢへコンテンツデータをコピー（複製）ではなく譲渡する場合には、メディアＡ側から暗号化鍵情報ＥA(G1)及び暗号化コンテンツデータＥG1(X)の内の少なくとも一方を消去する。

【００４０】また、図３（１）に示す方法と実現する記録装置としては、メディアＡ側において、一旦第１の暗号化コンテンツ情報ＥA(X)の暗号を解き、メディアＢ側から出力されたメディアＢのＩＤ＝Ｂを１Ｄ鍵としてコンテンツ情報を再暗号化して第２の暗号化コンテンツ情報ＥB(X)を得、その第２の暗号化コンテンツ情報ＥB(X)をメディアＢ側に出力させ、第２の暗号化コンテンツ情報ＥB(X)をメディアＢに記録させる記録手段を設ける。

【００４１】

【発明の効果】以上の通り、本発明によれば、不正な譲渡、複製を防止しつつ、メディアに記録されたコンテンツデータをユーザー間で譲渡、複製することを可能とし、必ずしも課金管理機関、データ管理センター等に接続しなくともユーザーがコンテンツデータを手に入れることを可能とする。また、この発明によれば、1人のユーザーが複数のメディアを持っていた場合、そのメディア間でデータの譲渡、複製を行えるシステムを提供できる。さらには、常に暗号化されたセキュリティの高い状態でコンテンツデータを譲渡、複製することができる。

【図面の簡単な説明】

【図１】一実施例に用いるデータ配信時の暗号化を説明するための図である。

【図２】一実施例の構成例を示す図である。

【図３】一実施例の機能説明図である。

【図４】一実施例の他の機能説明図である。

【図５】一実施例のメディア内のデータ構造図である。

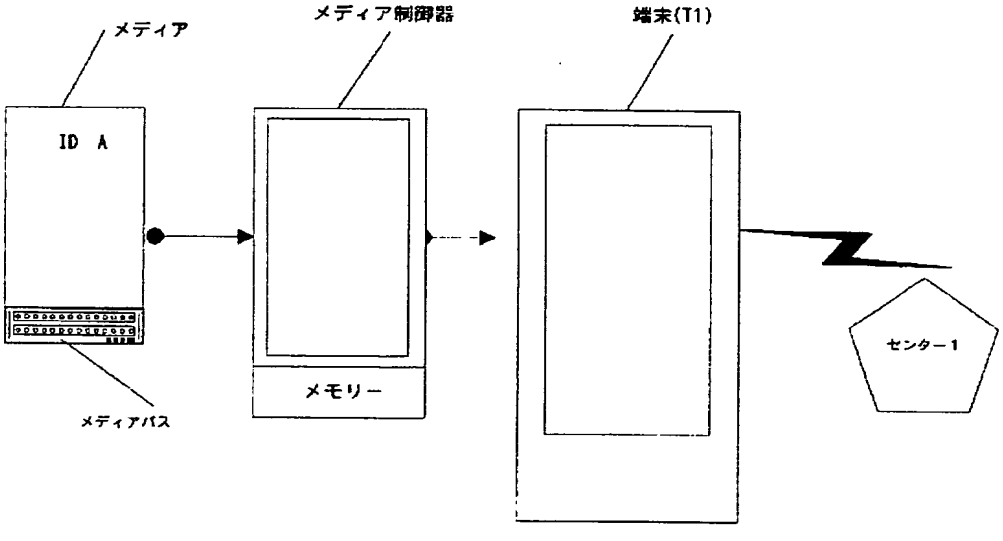
【図６】一実施例の詳細構成を示すブロック図である。

【符号の説明】

２１　メディア制御器
５１　モード設定部
５２　鍵暗号化部
５３　メディアID読み取り部
５４　暗号化鍵情報書き込み部
５５　暗号化鍵情報読み取り部
５６　暗号化鍵復号部
５７　暗号化コンテンツデータ復号部
５８　鍵メモリー

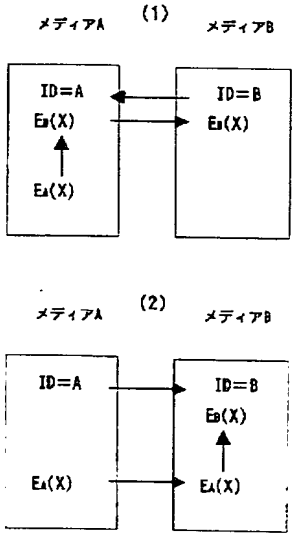
【図２】

図２



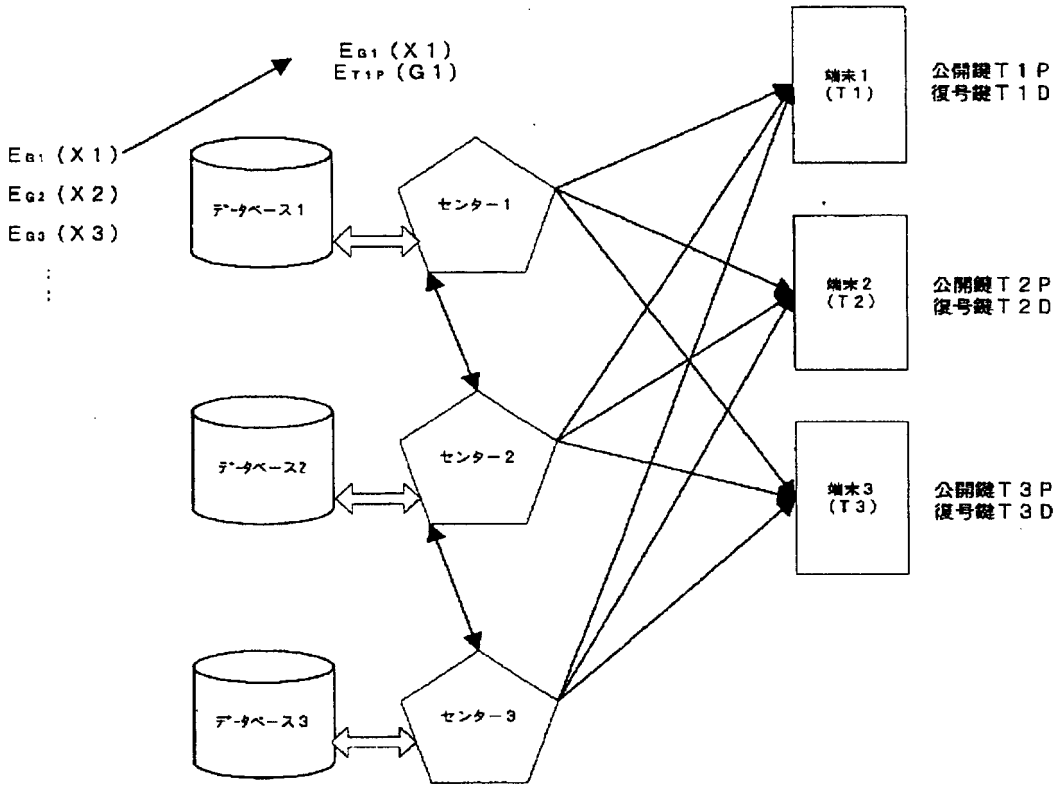
【図３】

図３



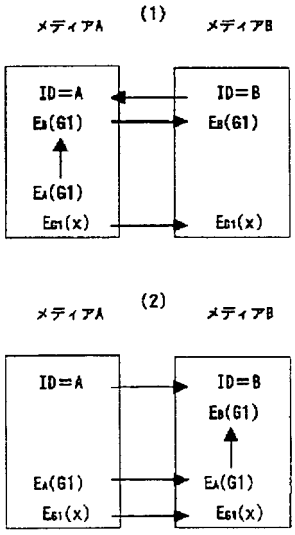
【図１】

図1



【図４】

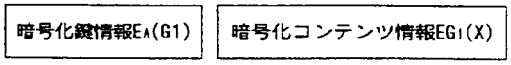
図4



【図５】

図5

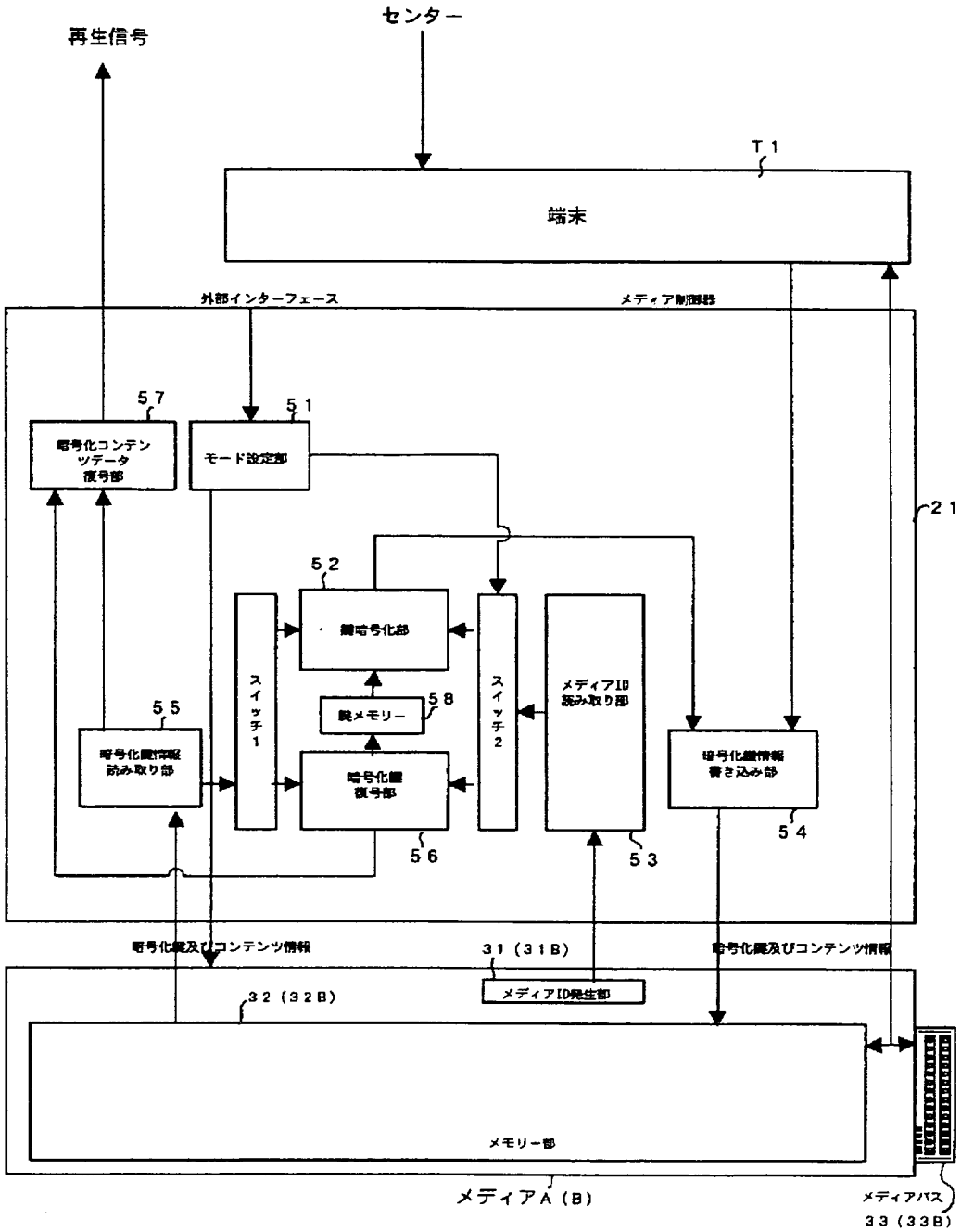
メディア内データ構造



６４ビット

【図６】

図６


センター
再生信号
T 1
端末
外部インターフェース
メディア制御器
5 7
5 1
暗号化コンテンツデータ復号部
モード設定部
2 1
5 2
鍵暗号化部
スイッチ1
スイッチ2
メディアID読み取り部
5 8
鍵メモリー
5 5
暗号化鍵情報読み取り部
暗号化鍵復号部
暗号化鍵情報書き込み部
5 4
5 6
5 3
暗号化鍵及びコンテンツ情報
3 1 （3 1 B）
暗号化鍵及びコンテンツ情報
メディアID発生部
3 2 （3 2 B）
メモリー部
メディアA（B）
メディアバス
3 3 （3 3 B）